Presented at the 5th International Association for the Advancement of Space Safety Conference in Versailles, France – October 17-19, 2011

Achieving the Proper Balance Between Crew & Public Safety

Paul Wilde [(1)], John Gowan [(2)], Ray Silvestri [(3)], Benjamin Stahl [(4)] & Paul Rosati [(5)]

[(1)] *Federal Aviation Administration, Johnson Space Center, Houston, TX, 77058 USA*
Email: paul.d.wilde@nasa.gov

[(2)] *National Aeronautics & Space Administration, Johnson Space Center, Houston, TX, 77058 USA*
Email: john.w.gowan@nasa.gov

[(3)] *National Aeronautics & Space Administration, Johnson Space Center, Houston, TX, 77058 USA*
Email: raymond.t.silvestri@nasa.gov

[(4)] *National Aeronautics & Space Administration, Johnson Space Center, Houston, TX, 77058 USA*
Email: benjamin.a.stahl@nasa.gov

[(5)] *Air Force 45th Space Wing, Patrick Air Force Base, FL 32925 USA*
Email: paul.rosati@patrick.af.mil

ABSTRACT

A paramount objective of all human-rated launch and reentry vehicle developers is to ensure that the risks to both the crew onboard and the public are minimized within reasonable cost, schedule, and technical constraints. Past experience has shown that proper attention to range safety requirements necessary to ensure public safety must be given early in the design phase to avoid additional operational complexities or threats to the safety of people onboard, and the design engineers must give these requirements the same consideration as crew safety requirements. For human spaceflight, the primary purpose and operational concept for any flight safety system is to protect the public while maximizing the likelihood of crew survival.

This paper will outline the policy considerations, technical issues, and operational impacts regarding launch and reentry vehicle failure scenarios where crew and public safety are intertwined and thus addressed optimally in an integrated manner. An overview of existing range and crew safety policy requirements will be presented. Application of these requirements and lessons learned from both the Space Shuttle and Constellation Programs will also be discussed. Using these past programs as examples, the paper will detail operational, design, and analysis approaches to mitigate and balance the risks to people onboard and in the public. Crewed vehicle perspectives from the Federal Aviation Administration and Air Force organizations that oversee public safety will be summarized as well. Finally, the paper will emphasize the need to factor policy, operational, and analysis considerations into the early design trades of new vehicles to help ensure that both crew and public safety are maximized to the greatest extent possible.

1. INTRODUCTION

For general space launch and reentry vehicles, a key component in design and operations is range safety. The vehicle developer is responsible for ensuring the vehicle meets range safety requirements as set forth by the governing launch range. Human-rated vehicles offer a unique design challenge in that crew risk must also be taken in to account along with public risk. In many cases, the optimal design solution to minimize public risk is non-optimal with regard to crew risk. This paper details current requirements on public and crew safety. It also shares key trades from the Space Shuttle and Constellation Programs as well as lessons learned from the Federal Aviation Administration (FAA) and Air Force (AF) 45th Space Wing regarding crew and public risk and the balance between the two.

2. CURRENT RANGE SAFETY REQUIREMENTS

2.1 AFSPC Range Regulations: The Headquarters (HQ) Air Force Space Command (AFSPC) operates the AFSPC ranges: 30th Space Wing [Western Range] at Vandenberg Air Force Base (VAFB), California and the 45th Space Wing [Eastern Range (ER)] at Patrick Air Force Base, Florida. The AFSPC ER is currently the only U.S. range supporting crewed space flight. As specified in AFSPC Instruction (AFSPCI) 91-701 [1], the AFSPC Commander (AFSPC/CC) is responsible for establishing range safety policy for AFSPC ranges. HQ AFSPC is responsible for establishing common range safety user requirements as outlined in AFSPC Manual (AFSPCMAN) 91-710, Range Safety User Requirements [2], for the AFSPC space wings to implement and enforce.

AFSPCMAN 91-710 defines responsibilities and authorities; delineates policies, processes, and approvals, and approval levels for all activities from or onto AFSPC ranges. These activities include the life cycle of launch vehicles and payloads from design concept, test, checkout, assembly, and launch to orbital insertion or impact. Currently all U.S. crewed space flight vehicles are launched from the ER, and therefore all crewed space flight programs must ultimately comply with AFSPCMAN 91-710 regarding public safety requirements. The document defines range user responsibilities and describes AFSPC range safety and range user interfaces at both AFSPC ranges. A range user is any individual or organization that conducts or supports any activity on resources (land, sea, or air) owned or controlled by AFSPC ranges. Example organizations include the Department of Defense (DoD), United States government agencies, civilian launch operators like the National Aeronautics and Space Administration (NASA), and foreign government agencies and other foreign entities. These organizations use AFSPC range

facilities and test equipment; conduct prelaunch and launch operations, including payloads to orbital insertion or impact; and/or require on-orbit or other related support. Therefore, when launching crewed space vehicles from the Kennedy Space Center, NASA is a range user of the ER, with sole responsibility for crew safety.

The responsibility for protecting the public, launch area, and launch complex personnel and resources is of paramount consideration in range launch operations. As a range user, NASA seeks to maximize both crew and public safety within the cost, schedule, and technical constraints placed on a given launch (and/or reentry) vehicle project / program. Therefore, when launching a crewed vehicle from an AFSPC Range, NASA must not only comply with the AFSPCMAN 91-710 requirements for public safety, but also with its internal NASA Procedural Requirements for crew safety. The Space Wing Commanders (SW/CCs) have overall authority and responsibility for public safety at AFSPC ranges as directed by the AFSPC/CC. This delegation is provided via the Major Command (MAJCOM) chain of command and Air Force Instruction (AFI) 91-202, The US Air Force Mishap Prevention Program [3].

It is the policy of the ranges to ensure that the risk to the public, launch area, and launch complex personnel and resources is managed to an acceptable level. This policy is implemented by employing risk management in three categories of safety: Public Safety, Launch Area Safety, and Launch Complex Safety. The range user is required to manage risk to the lowest level, consistent with mission requirements, and in consonance with AFSPC range launch risk guidance. Individual hazardous activities may exceed guidance based on national need after implementation of available cost-effective mitigation. It is the policy of the ranges to avoid the use of waivers. However, the Space Wing Commanders (SW/CC) have the authority to tailor or waive any requirement in AFSPCMAN 91-710. Based on national need, and the approval of the SW Commanders, non-FAA licensed launches may be permitted using a predicted risk above criteria as shown in Fig. 1 in accordance with AFI 91-217, Space Safety and Mishap Prevention Program [4].

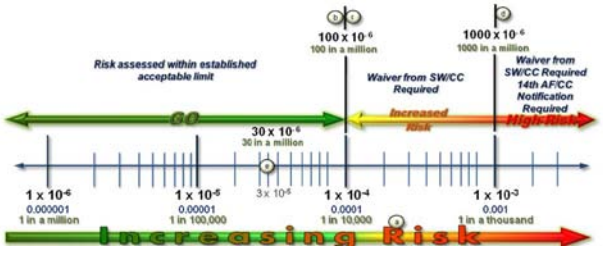

Figure 1. AFSPC Range General Public Aggregated Risk Criteria for Non-FAA Licensed Launches.

Refer to AFSPCI 91-701 for risk approval levels at the two AFSPC ranges. Range Commanders Council (RCC) Standard 321-10 [5] provides relevant background information on launch risk acceptability. AFI 91-217 provides overarching space safety, mishap prevention and mission effectiveness guidance for acquisition, testing, and operations of terrestrial, launch, orbital and kinetic/directed energy space systems. This document establishes risk criteria for launch through orbital insertion and reentry risk criteria for each reentering object. It also establishes roles and responsibilities. From lift off to orbital insertion, SW/CCs have safety (personnel/asset protection) responsibilities. A U.S. consensus standard, RCC 321-10, defines orbital insertion in the following manner: "orbital insertion occurs when the vehicle achieves a minimum 70 nm perigee based on a computation that accounts for drag." This definition has been accepted by the Air Force as documented in a recently released Interim Change to AFI 91-217. After orbital insertion, safety (personnel/space asset protection) becomes the sole responsibility of the range user, such as NASA. This is further documented in the National Space Policy.

In order to effectively implement AFSPC Range Safety Policies certain components have been identified as Range Safety Critical Systems, which include all airborne and ground subsystems of the Flight Safety System (FSS). The FSS consists of airborne and ground Flight Termination Systems (FTSs), airborne and ground Range Tracking System (RTS), and the Telemetry Data Transmitting System (TDTS). The ground FSS also includes any hardware or software system, subsystem, or elements thereof that could 1) prevent the Mission Flight Control Officer (MFCO) from stopping the launch of a vehicle, determining the performance of a nominal or non-nominal launch vehicle, or commanding flight termination action; or 2) cause unauthorized issuance of FTS commands.

All AFSPC Range Safety Critical Systems shall be designed to ensure that no single point of failure, including both hardware and software, will deny the capability to monitor and terminate, or result in the inadvertent termination of, a launch vehicle or payload, as applicable. When possible, AFSPC Range Safety critical systems shall be designed to be dual fault tolerant against failure in hardware and software and still provide overall system redundancy.

The reliability requirements of the FSS are as follows:

- The overall airborne and ground FTS reliability goal is 0.9981 at the 95 percent confidence level.
- The airborne FTS reliability goal shall be a minimum of 0.999 at the 95 percent confidence level for global positioning systems and 0.95 at the 95 percent confidence level for transponder systems.
- The ground FTS shall have a reliability of 0.999 at the 95 percent confidence level for a 4-hour duration, as required.

FTS functional requirements ensure that when initiated, whether by command from a MFCO or other means, such as automatically in the event of a vehicle failure, an FTS shall:

- Ensure the flight-terminated vehicle's debris impact, resulting from residual lift or drift under worst case wind conditions, will not endanger any protected area.
- Be irrevocable upon termination initiation.
- For each propulsion system that has the capability of reaching a protected area, terminate the flight and/or render the system incapable of propulsion. This includes each stage and any strap-on motor or propulsion system that is part of any payload.
- Destroy the pressure integrity of any solid propellant system and terminate all thrust or ensure that any residual thrust causes the propulsion system to tumble without significant lateral or longitudinal deviation in the impact point.
- Disperse any liquid propellant, whether by rupturing the propellant tank or other equivalent method.

> Shutdown and/or parachute systems may be used in lieu of rupturing propellant tanks if the risks posed by an intact impact are acceptable. Determination of shutdown-only systems will be range and vehicle dependent.

In order to control potential errant vehicle flight AFSPC Range Safety shall verify that all launch vehicles launched from or onto the ranges have a range-approved method of controlling errant vehicle flight to meet the objective of minimizing risks to the public, launch area, and launch complex personnel and resources. Normally, control systems on launch vehicles using the ranges shall consist of an airborne FSS that shall meet all the requirements of volumes 2 and 4 of AFSPCMAN 91-710. A thrust termination system may be considered as an alternative to an FSS. However, quantification of risks shall be determined and the requirements in Volume 2 shall still be met. The alternative thrust termination concept and design shall be approved by the SW Commander. AFSPC Range Safety shall establish flight termination criteria and AFSPC Range Safety mission flight rules to ensure that operations do not exceed acceptable public safety limits.

AFSPC Range Safety shall establish and control hazardous launch areas and procedures to protect the public on land, on the sea, and in the air for each launch and launch vehicle. This is accomplished by ensuring that no intact launch vehicle, scheduled debris or payload, or launch vehicle and payload subsystems shall be allowed to intentionally impact on land, except in the launch area inside the impact limit lines. Flight paths and trajectories shall be designed so that normal impact dispersion areas do not encompass land. Safety margins shall be used to avoid overly restrictive flight termination (destruct) limits. AFSPC Range Safety policy may allow errant launch vehicles to fly to obtain maximum data until they would present an unacceptable risk to the public or until AFSPC Range Safety can no longer control the launch vehicle.

In accordance with the 2011 Commercial Space Launch Act [6], the FAA has responsibility for public safety of commercially licensed launches. The AFSPC Range Safety requirements in AFSPCMAN 91-710 have been written with the intent of achieving commonality with the FAA requirements. The FAA performed launch site safety assessments (LSSAs) of the two AFSPC national launch ranges and determined the level of safety obtained by the existing range safety processes to be adequate. The FAA will not require a license applicant to demonstrate the adequacy of the range services it proposes to use if the applicable LSSA included those services and if those services remain adequate. SW Commander discretion to accept higher risk for the launch of government payloads does not apply to commercially licensed launches without a range user obtaining relief from the FAA [7].

2.2 FAA Regulations: Current FAA regulations focus on public safety requirements for commercially licensed launch vehicles because the Commercial Space Launch Amendments Act (CSLAA) of 2004 [8] authorized the FAA to "issue regulations governing the design or operation of a launch vehicle to protect the health and safety of crew and space flight participants" only to the extent necessary "to protect the public health and safety, safety of property, national security interests, and foreign policy interests of the United States," or to address "design features or operating practices that have resulted in a serious or fatal injury" or "contributed to an unplanned event or series of events during a licensed or permitted commercial human space flight that posed a high risk of causing a serious or fatal injury." In response to the CSLAA, the FAA issued the regulations in 14 CFR Part 460 [9]: a relatively sparse set of requirements for commercial human space flight that includes rules on crew qualifications and training, informed consent for crew and space flight participants, financial responsibility and waivers of liability. A "space flight participant" was defined in the CSLAA as "an individual, who is not crew, carried aboard a launch vehicle or reentry vehicle;" the term "passenger" carries legal implications that are not appropriate for transportation under the informed consent paradigm. The FAA's current regulations are intended to provide an acceptable level of safety to the general public and ensure individuals onboard are aware of the risks associated with a launch or reentry. The FAA does not prescribe any limits on the risk accepted by individuals onboard a commercial launch or reentry vehicle. Instead, the FAA requires (in §460.9 for crew and in §460.45 spaceflight participants) an operator to inform any spaceflight participant or individual serving as crew in writing that the United States Government has NOT certified the launch or reentry vehicle as safe for carrying human beings. In contrast to the current FAA requirements for commercial human space flight, 14 CFR Part 417 [10] provides a relatively extensive set of requirements aimed at ensuring public safety during an Expendable Launch Vehicle (ELV) launch, including a quantitative public risk acceptability criteria (in §417.107) of 3E-5 Expected Casualties (E_C) and a maximum individual risk of 1E-6 Probability of Casualty (PC) for each source of hazard from lift-off to orbital insertion. The current FAA regulations for a Reusable Launch Vehicle (RLV) launch or reentry, 14 CFR Part 431 [11], include the same quantitative public risk acceptability criteria for the entire mission, from lift-off through landing. However for orbital missions, the FAA has applied the public risk criteria limits separately for launch and reentry [12]. Thus, all FAA licensed launches and reentries are required to comply with quantitative public risk criteria that limit collective and individual risks.

The Commercial Space Launch Amendments Act of 2004 also authorizes the FAA to propose regulations for the design or operation of any commercially licensed crewed launch vehicle to protect the health and safety of crew and space flight participants beginning in December of 2012. Thus, the FAA seeks to understand past experiences, lessons learned, as well as potentially effective and innovative approaches related to the integration of crew and public safety requirements.

3. CURRENT CREW SAFETY REQUIREMENTS

NASA has established crew safety requirements for crew transportation missions to the International Space Station. The Loss of Crew (LoC) requirements established for the ascent and entry phases are documented in the ISS Crew Transportation and Services Requirements Document [13]. In addition to the LoC requirements, the agency has a document, NASA Procedural Requirements (NPR) 8705.2B [14], that addresses procedures and technical requirements to manage the crew safety risk associated with human spaceflight. NPR 8705.2B applies to the development and operation of crewed space systems developed by NASA used to conduct NASA human spaceflight missions. This NPR may apply to other

crewed space systems when documented in separate requirements or agreements. Section 3.6 of the NPR specifically addresses high level crew survival and abort requirements.

4. LESSONS FROM SPACE SHUTTLE PROGRAM

The Space Shuttle Program provides 30 years of history and lessons learned for both crew and public safety, but until now, not a lot of attention had been placed on capturing the lessons learned regarding the interaction between the two. In some instances, certain Shuttle design features can place crew and public safety at odds with each other. While these risks to the crew and public have been carefully mitigated and balanced for the Space Shuttle Program, it required countless hours of analysis and discussion in order to craft an acceptable set of operational rules and procedures. In other words, by not placing special emphasis on the crew versus public safety balance during the design phase, the responsibility for finding an acceptable balance fell on the shoulders of the vehicle operators and AFSPC Range Safety authorities. In addition, a truly optimal balance between crew and public safety could not be achieved without significant and costly redesigns. A few examples from the Space Shuttle Program include the addition of a secondary impact limit line, the removal of the External Tank Flight Termination System (FTS), External Tank disposal for certain contingency aborts, and the compromised Orbiter flight rules for Space Shuttle reentry.

4.1 Addition of a Secondary Impact Limit Line: To protect the public and critical assets in the launch area vicinity, the ER establishes an Impact Limit Line (ILL) that serves as a boundary past which debris with greater than a ballistic coefficient of 3 psf is not permitted to penetrate in the event of a vehicle malfunction and subsequent breakup. Destruct criteria are established to ensure the ILL is not violated for an errant launch vehicle, and for all launch vehicles except the Space Shuttle, there is only one ILL. An exception to the single ILL philosophy was granted for the Space Shuttle due to crew safety concerns and the unique nature of the Shuttle's "autoloft" guidance logic for abort scenarios. This exception was made to account for the fact that the Space Shuttle will intentionally modify the pitch profile of the vehicle and steepen the trajectory in first stage for the loss of one or more Space Shuttle Main Engines (SSMEs). This lofting is necessary to provide the crew with an abort capability that would not otherwise exist, thereby dramatically increasing their chances of survival. However, the increased lofting results in a violation of the primary ILL despite the vehicle remaining in control, continuing to head downrange and flying the intended abort profile. Hence, a secondary ILL was established for the Shuttle that is further west than the primary line.

For the Space Shuttle ascent, flight termination would only be implemented in response to a primary ILL violation if the vehicle has exceeded the controllability limits, which are defined as pitch or yaw rates in excess of 5 deg/sec for more than 5 seconds. If neither the flight control team in the Mission Control Center (MCC) in Houston nor the MFCO at Cape Canaveral Air Force Station can positively determine the controllability status of the vehicle, the MFCO would assume the Shuttle is still in control and would permit a primary ILL violation in accordance with the Space Transportation System (STS) flight rules. However, regardless of the vehicle's controllability status, the STS flight rules did not allow a violation of the secondary ILL without destruct action being triggered in response unless confirmation was received that the trajectory deviation was due to the loss of two SSMEs and the slight violation occurred late in first stage. Additionally, for the loss of two SSMEs, the vehicle must meet the following criteria: 1) remain in control, 2) stay within predetermined flight azimuth envelopes, 3) transition through maximum dynamic pressure without vehicle breakup, and 4) still have its instantaneous impact point (IIP) moving downrange. If any of these criteria were not met, then destruct action would be taken for this dual SSME failure scenario.

The need to add a secondary ILL for the Shuttle was due to inherent design features, or lack thereof, that should have taken range safety requirements into account during the early design phase of the Space Shuttle. For example, the lack of a first stage crew escape system resulted in a complex set of operational flight rules and procedures to mitigate any increased public risk associated with the vehicle being permitted to fly past the primary ILL. For future crewed launch vehicles, the ER plans to permit only one ILL. Fortunately, new launch vehicle design concepts have all included a first stage abort capability that will be designed to safely extract the crew module in the event of a major failure and/or FTS destruct action. Even with this first stage escape capability, careful consideration regarding the balance between crew and public safety still needs to factored into early design trades to ensure that both crew and public safety requirements are being met.

4.2 Removal of the External Tank FTS: Following the STS-51L Challenger accident in 1986, NASA began a number of studies analyzing the breakup process of the Shuttle Solid Rocket Boosters (SRBs) from command destruct as well as the resulting impact on the neighboring External Tank (ET). "One of the recommendations of the Presidential Commission investigating the Challenger accident was to remove the ET destruct system, a move fully endorsed by the Astronaut Office" [15]. The ensuing studies showed that a command destruct of the Shuttle SRBs would result in debris penetration and breakup of the liquid hydrogen (LH2) tank even if the ET FTS was removed. The damage to the liquid oxygen (LOX) tank was less certain, and therefore an initial decision was made by NASA and the 45th Space Wing to only remove the FTS on the LH2 portion of the tank. This initial modification to the ET FTS occurred in 1992 and was first implemented on STS-47. However, several years later, another set of analysis studies and discussions resulted in the removal of the FTS on the LOX tank as well, which thereby eliminated all command destruct capability on the Shuttle ET. To remove the FTS from the LOX tank, a more integrated risk assessment was performed for both the launch area as well as the downrange overflight region. "Results clearly indicated that removal of the LOX tank RSS neither dramatically increased total risk levels nor created risk levels in excess of the allowable limits. This analysis concluded that public and workforce risk are within acceptable limits for Shuttle launches with the LOX tank RSS ordinance removed" [16].

NASA's primary motivations for removing the FTS on the ET were the reduction in vehicle weight and the reduced risk to both the crew and vehicle from a low-probability inadvertent FTS destruct action. However, both NASA and the Air Force were concerned about public safety and wanted to ensure that the removal of the ET FTS would not significantly increase

the expectation of casualty (E_C) values, which remain the primary criterion for evaluation of public risk. For first stage flight, the primary concern was the possible overpressure that may result from an intact LOX and/or LH2 tank impacting the launch area following a breakup event. As discussed earlier, the LH2 tank was shown to break apart once the SRB FTS was invoked, and the risk associated with an intact LOX tank impact was shown to be relatively small. For second stage flight, NASA and the Air Force agreed that thrust termination (i.e. shutdown) of the three liquid fueled SSMEs would provide a similar level of safety as a command destruct action. This argument was further advanced by analysis results showing that the ET would experience aero-thermal breakup on reentry for the majority of SSME failure times in second stage. In the eyes of range safety authorities at the time, this combination of SSME shutdown capability and likely ET rupture on reentry was enough to satisfy the intent of the public risk requirements during second stage flight.

The concept of using thrust termination (i.e. SSME shutdown) in lieu of FTS command destruct required the incorporation of several mitigation techniques that needed to be implemented into future Shuttle operational procedures. The first modification involved reevaluating and re-designating the destruct lines placed along the east coast of the U.S. and Canada. These lines no longer represented the point at which destruct action needed to be taken but instead signified the point at which a manual SSME shutdown needed to occur in order to prevent the ET from impacting land. In addition, one of the operational roles of the astronauts onboard the vehicle changed as well. With their responsibility to terminate thrust should the need arise, "the flight crew commander and pilot become agents of the 45th Space Wing Commander for public safety during the portion of flight after solid rocket booster separation and prior to main engine cutoff" [17]. In fact, an entire set of flight rules, operational procedures, and training materials needed to be drafted or rewritten to reflect the new operational paradigm where the flight crew and the MCC flight control team were now directly responsible for the real-time execution of AFSPC Range Safety actions during second stage ascent.

This is one example where the slight increase in public risk was deemed to be acceptable by both NASA and Air Force authorities in favor of the reduction in crew risk and enhancement of the vehicle's performance capabilities (i.e. reduction in vehicle weight). In other words, the benefits to crew safety and the launch vehicle program outweighed the added risk to the public, which was mitigated through the implementation of several operational flight rules and procedures.

4.3 External Tank Disposal for Contingency Aborts: Although the Shuttle does not have a crew escape system for the ascent phase of flight, it is designed to keep the crew and vehicle intact for abort scenarios involving a single SSME shutdown. For multiple SSME failures, the vehicle must perform a "contingency abort" that is intended to either land the Orbiter at an emergency runway location or achieve safe conditions for the crew to bailout during the glided flight phase. These "contingency aborts" (for multiple engine failures) do not include the design protection or continuous abort coverage that is associated with "intact aborts" (for single engine failures), and therefore have a lower chance of success. Once the launch vehicle reaches second stage, the likelihood of the crew surviving multiple SSME failures begins to increase as more (and safer) abort options become available. The risk to the public is also diminished in second stage due to the large downrange velocity of the vehicle, the ability to terminate thrust by shutting down the SSMEs, and the vehicle's relatively distant proximity to the heavily populated areas along the U.S. coastline. Despite these factors, there are contingency abort scenarios where the Shuttle's External Tank could pose a risk to downrange landmasses along the east coast of the U.S., Newfoundland, or in parts of Eurasia. For these off-nominal scenarios, the flight control team in the MCC is placed in the precarious position of trying to protect the crew while at the same time ensuring that range safety criteria are not being violated.

One example involves a scenario that is occasionally practiced by the crew and the MCC flight control team during integrated training simulations. The failure scenario involves the loss of one SSME during first stage with another engine that is "sick" (e.g. leaking Helium, etc.). The sick engine for this scenario is predicted to shutdown early enough to prevent the vehicle from performing an intact abort. As a result, a contingency abort known as an East Coast Abort Landing (ECAL) is required. The ECAL guidance logic is used to try to steer the vehicle closer to the coast during powered flight in an attempt to land at one of the ECAL runways. By steering closer to the coast, however, the vehicle begins to approach the range safety line established to protect the U.S. east coast from possible impact by the External Tank. The MCC flight control team will monitor the situation and instruct the crew to perform an immediate manual shutdown of all SSMEs in the event the range safety line is being encroached. By performing this manual shutdown earlier than necessary to reach an ECAL runway, the crew and the MCC flight control team avoid endangering the public but will likely place the crew in a situation requiring them to bail out during the glided flight phase.

The aforementioned example illustrates a case where both crew and public risk are pushed near their maximum acceptable limits. It would be more desirable from a public safety standpoint if the vehicle did not intentionally steer towards the coast following the SSME failures. In contrast, it would be more desirable from a crew safety standpoint to fly past the range safety line and shutdown the engines a later point in the trajectory, thereby improving the vehicle's chances of safely reaching a runway. In the end, the operational procedures were crafted such that the crew was given the maximum allowable leeway to deviate towards the coast without violating the predetermined range safety criteria. However, it is important to note, as seen from this example, that extra conservatism in AFSPC Range Safety criteria or crew risk mitigations can lead to a situation where the optimal balance is not achieved because conservatism on one side or the other biased the solution.

4.4 Compromised Orbiter Flight Rules for Reentry: The Columbia accident highlighted the need for NASA to better understand the risk to people on the ground for the Space Shuttle entry phase. The Columbia Accident Investigation Board (CAIB) observed that NASA should take steps to mitigate the risk to all persons and property from Orbiter entries. As a result, NASA developed a set of flight rules and operational procedures to handle situations where the Orbiter may be "compromised," defined as any condition or failure that substantially reduces the likelihood of a nominal entry and landing" [18]. Even for a standard entry, certain cross-ranges

(i.e. ground-track approaches) "will be avoided in order to abate the risk to the general public" assuming all other nominal "landing site selection priorities for weather, consumables, runway conditions, and entry constraints" are satisfied. For a compromised Orbiter, the operational considerations for landing site selection become more weighted towards protecting the public since a failure or damaged condition has already occurred, resulting in a higher likelihood of vehicle breakup during entry. By prioritizing landing sites differently and avoiding certain cross-ranges, the risk to the public for a compromised Orbiter is reduced by approximately one order of magnitude when compared to the highest risk opportunity to Kennedy Space Center (KSC).

For a nominal entry, KSC is always given priority over the other two primary landing sites, Edwards and Northrop, due to lower vehicle turnaround costs. Edwards is then prioritized above Northrop, which has only been used once in the program's history and is rarely even considered during nominal real-time operations. Crew safety also factors into this landing site prioritization since the crew and flight control team practice for a landing at KSC or Edwards far more often than Northrop. There is also inherent risk in going to a landing site that has only been utilized once and is not as familiar to the crew or flight control team as the other two primary sites. Yet for a compromised Orbiter scenario, Northrop is given priority over KSC and Edwards in order to "abate the public risk to the extent feasible." In addition, lower public risk ground-track approaches are emphasized for the compromised Orbiter scenario. However, by performing orbit adjust maneuvers or forgoing good deorbit opportunities in favor of more favorable public risk approach trajectories, the crew risk inevitably is higher.

This example illustrates the need to balance crew and public risk not only during the ascent phase but during vehicle reentry as well. For the Space Shuttle Program, an appropriate balance was achieved by prioritizing landing sites and selecting ground track approaches with a more public safety focus in the event the vehicle becomes damaged or experiences a failure at an earlier stage in the mission. Achieving this balance required considerable analysis and discussion during the Space Shuttle "return to flight" period and should have been addressed at an earlier stage in the program.

5. LESSONS FROM CONSTELLATION PROGRAM

The Constellation Program performed many assessments on crew and public risk in requirements drafting, design of the vehicles, and the overall concept of operations. A few key assessments and findings are detailed below.

5.1 Breakup Event Environment: One of the key products that impact both public and crew safety assessments is the categorization of the environment resulting from breakup scenarios. The prime crew risk outcomes (environment) of a breakup event are overpressure, thermal radiation and debris. Prime initiators of breakup are FTS initiation, explosion, and aerodynamic and thermal load violations. LoC and abort effectiveness (i.e. given the abort, how successful is it) assessments are done with consideration to spacecraft vulnerability using these environments. Of the crew risk breakup outcomes, AFSPC Range Safety assessments primarily consider the debris environment. The data requirements for the debris environment (catalog) are identical to support both crew and public risk assessments as the physics and the goals (accurate, high fidelity) of defining the environment are the same. The basic contents of a debris catalog are piece count, mass, aerodynamic characteristics (ballistic coefficient), velocity and variability (min/max or distribution of the preceding parameters). The timeline of interest does vary between the two assessments. AFSPC Range Safety assessments are ground focused based on public safety concerns, with consideration for risk to commercial aircraft. Crew safety assessments have a near field relative focus and are spacecraft relative with some far field implications (thermal radiation impacts on parachutes). Although the application of the breakup environment can differ between assessments, the goal of a program should be to establish a single product per event and breakup mode that can be used for both crew and range safety assessments.

5.2 Ares FTS Delay Timer: As specified in NASA NPR 8715.5 [19], any vehicle, stage or payload with propulsive capability that poses elevated risk to the public shall have an FTS to satisfy range safety requirements. This requirement is also in the AFSPC Range Safety governing document AFSPCMAN 91-710. The FTS is designed to render each propulsive system that has the capability of reaching a protected area incapable of propulsion. This includes each stage and any strap-on motor of the propulsion system that is part of any payload. The timing of the FTS action has been shown to impact crew survivability for solid rocket motor propulsive vehicles due to the overpressure, debris and thermal radiation impacts of the launch vehicle destruction. Most FTS designs act immediately upon receipt of the destruct command by terminating thrust and dispersing propellants. However, immediate FTS action on a crewed vehicle poses a significant threat to the crew since additional time is needed for the crew to escape the exploding launch vehicle. In order to minimize risk to the crew, the Constellation Program planned to employ an onboard FTS delay timer. This hardware fuse-based timer would insert a delay from when the FTS fire command was received onboard to when the destruct mechanism was fired. This would allow the crewed launch abort vehicle (LAV), consisting of the combined Crew Module (CM) and Launch Abort System (LAS), to depart the launch vehicle and safely escape the explosion and resulting debris field. However, the negative by-product of inserting an onboard FTS delay timer is the transfer of increased risk to the public due to the longer flight time associated with the malfunctioning booster. Optimization of the FTS delay time from a crew risk perspective is detailed in Section 5.2.1. Public risk concerns associated with the FTS delay timer are detailed in Section 5.2.2. Section 5.2.3 summarizes the trade between crew and public risk with FTS delay time.

5.2.1 FTS Delay Time Optimization for Crew Risk: The Orion LAS was designed to meet a very basic launch vehicle re-contact requirement stating the LAV must be greater than 175 ft away from the center of gravity of the launch vehicle 3 seconds after abort. This requirement did not guarantee success against debris strikes and in-depth analyses had not yet been performed to quantify the risk. Therefore the Constellation Program documented and tracked a risk of unacceptably high loss of crew due to Orion exposure to the debris field generated by either FTS activation or Ares structural break-up. In order to quantify and minimize that risk, analyses were performed to determine the optimal FTS delay time for crew safety.

During the design and development phase of the Constellation program, several iterations were performed on ascent abort debris risk to the crew. Efforts were focused on aborts during first stage flight since this portion of flight was nearest to the populated coast and the solid propellant first stage booster was incapable of being shut down. For these reasons, first stage flight posed the greatest risk for FTS action. Early analyses focused on vehicle re-contact. Later analyses evolved into more complex debris strike analyses. Analysis was performed by teams from NASA's Ames and Johnson Space Centers, ATK in Utah, and the 45th Space Wing at Cape Canaveral (i.e. the AFSPC range where the vehicle would launch from).

In an effort to capture the full suite of possible abort trajectories, on-track aborts as well as malfunction turn aborts were analyzed for re-contact and debris strike probability. On-track aborts are aborts from a launch vehicle that still has full Thrust Vector Control (TVC) control and is flying the target trajectory. Malfunction turn aborts are aborts from a launch vehicle that has experienced a failure resulting in a noticeable trajectory deviation.

Results concluded that the LAV and current LAS design were able to meet the Orion 175 ft re-contact requirement as specified but with little margin. On-track and actuator fail-in-place aborts were the limiting cases since the continuously thrusting launch vehicle eventually chases down the LAV and passes by. The actuator fail-to-null and hard-over trajectories resulted in a malfunction turn or tumbling launch vehicle that eliminated the chaser effect. Additionally, during the transonic and high dynamic pressure (high Q) phases of the ascent, the departing LAV is more quickly decelerated by the atmosphere. This further exacerbates the re-contact and debris concern. The Ares FTS delay time was optimized based on these limiting on-track and fail-in-place transonic and high Q cases. The delay provided sufficient time for the LAV to depart the launch vehicle and achieve safe separation distance, but not so much time to allow the launch vehicle to eventually chase down the LAV and destruct in close range. At the time of program cancellation, the Constellation Program had not received concurrence for the FTS delay time from the AFSPC range where the vehicle would be launched.

Note that the static FTS delay time was optimized for a scenario where commanded FTS action would trigger the abort. A more likely scenario was that the abort would be triggered via onboard anomaly detection. In this scenario, a period of time elapses while the MFCO confirms the vehicle should be destroyed and then the MFCO sends the command to destruct the vehicle. As a result, the vehicle could have an FTS breakup event at a non-optimal time from a crew risk perspective. At the time of cancellation, the Constellation Program was discussing the option of automatically firing the FTS when a LAS abort was declared in order to guarantee the vehicle would be destroyed at the optimal time. This would prevent occurrence of the previously mentioned scenario where the MFCO destructs the vehicle as it passes within close range of the LAV and would also eliminate the MFCO (i.e. human-in-the-loop) from having to manually destroy the booster since this would be done automatically onboard. This type of abort-initiated, automatic destruct action could result in an overall improvement to both crew and public safety if properly designed and implemented (i.e. no additional delay time beyond the "normal" MFCO FTS activation delay time).

5.2.2 Public Risk Concerns with an FTS Delay Timer: Although application of additional FTS delay provides the crew with an opportunity for safe escape of a destructing launch vehicle, it will result in an increase in risk to the public in the event of an errant-flying vehicle. For aborts early in first stage flight when the launch vehicle is still near the east coast of Florida, an additional delay of FTS activation may result in the debris impact point traversing over land to a populated area. As mentioned earlier, the fuse-based FTS delay timer onboard is added onto other delays that may be present in the onboard and ground systems used to invoke FTS destruct action. When MFCO delays (i.e. human reaction time), data latency, and other system delays are added to the fuse-based timer, the total delay time between the vehicle malfunction and the FTS destruct event could approach or exceed an unacceptable limit, past which the delay results in a violation of AFSPC Range public risk criteria (e.g. an E_C violation). Furthermore, the vehicle designers must ensure that the FTS hardware is located in a region of the structure that is robust enough to survive the aerodynamic loads imparted on the vehicle during a malfunction turn. As mentioned in Section 2.1, the FTS must be certified to 99.9% reliability with 95% confidence for both the nominal and off-nominal flight environment. There are concerns that if the delay in FTS activation is too lengthy, the vehicle could lose control and exceed structural loading limits during the time period between the initial vehicle failure and the time at which the FTS activated destruct occurs. In such a scenario, the MFCO may have commanded FTS action, but vehicle breakup or extreme environments could destroy the FTS or the destruct ordnance train during the delay period, thereby preventing the FTS from splitting the booster case and dispersing propellants. As a result of these factors, all FTS activation timing delays need to be closely analyzed from a public safety standpoint and would require prior approval from the AFSPC Range (i.e. 45th Space Wing), the vehicle is launching from before being implemented.

5.2.3 Balancing Crew and Public Risk with FTS Delay: The FTS delay time assessment provided a concrete example of the complexity in integrating crew and public risk for crewed launch vehicles using a solid rocket motor propulsive system. From a crew perspective, abort flight is safer if the launch vehicle is not destroyed. The capability of the LAV to avoid an intact solid rocket motor launch vehicle flyby was demonstrated via simulation. It can be argued that complete removal of the FTS system would maximize crew survivability in the event of an abort. In contrast, from a public risk perspective, the launch vehicle could be significantly safer if the FTS system destroys the launch vehicle as soon as an anomaly is detected. Each second of delay allows the vehicle impact point to propagate potentially closer to populated areas and allows the FTS system to be compromised due to structural and aerodynamic loads associated with the launch vehicle failure. FTS delay time was heavily discussed and analyzed throughout the life of the Constellation Program. In order to assure crew safety is optimized while protecting the public from an errant launch vehicle, efforts must be made to design a robust FTS system and abort logic that accounts for the post FTS action impacts on both LoC and public risk. For all future launch vehicle programs, the system designers will need to work closely with the AFSPC range where the vehicle will be launched to ensure any proposed design solutions are not only acceptable from a crew safety standpoint but also meet all public safety criteria set forth by the range.

5.3 Component Disposal for Ascent Aborts: Both Ares and Orion posed safety concerns with component disposal in the event of an abort. Section 5.3.1 details disposal concerns for Ares. Section 5.3.2 discusses Orion abort disposal concerns. Finally, Section 5.3.3 discusses the crew and public risk trades associated with abort disposal.

5.3.1 Ares Component Disposal: Launch to the ISS results in nominal overflight of Eurasia immediately prior to Main Engine Cut-Off (MECO). The Ares Upper Stage was designed to splash down in the Indian Ocean nominally, but for under-speed scenarios the Upper Stage could impact land. The Ares Project performed an entry analysis for under-speed or early MECO cases to quantify risk and protect for land impact. For Ares, the total overflight exposure begins approximately 10 seconds before nominal MECO when the vehicle impact point intercepts the western European coast. Fig. 2 illustrates the overflight risk for one ISS and two lunar mission trajectories. The colors correspond to varying early MECO times. For ISS launches at the close of the launch window, a brief 1-2 second overflight of Newfoundland also occurs. This concern is more apparent in abort scenarios, discussed below.

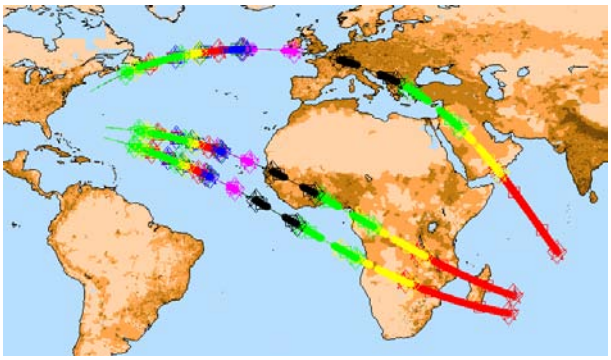

Figure 2. Ares Upper Stage splashdown locations for early MECO scenarios.

5.3.2 Orion Component Disposal for Abort Scenarios: Orion components also present a debris risk concern, albeit secondary to the Ares Upper Stage scenarios discussed previously. Orion LAS aborts occur predominantly in the open waters off the coast of Florida. Only an abort from the pad poses any concern, where the CM can drift back over land due to winds. It was anticipated that this area would be cleared for launch so no public risk would exist and Orion meets a 95% success criteria for landing in at least 10 feet of water even for pad abort cases with wind dispersions. However, Orion Service Module (SM) aborts posed a downrange disposal concern. An SM abort is an abort during second stage flight that relies on the Orion SM for translation and attitude control to target a safe orbit or an abort landing area in the North Atlantic Ocean. During an SM abort to a landing area, the Orion SM and Orion Docking Mechanism (DM) can contribute to the debris risk to the public. The primary concern for SM aborts is SM/DM impacts on Newfoundland or the Hibernia Oil Platform for aborts to the St. John's abort landing area. Abort landing areas are depicted in Fig. 3, along with the Downrange Abort Exclusion Zone (DAEZ), an area of the North Atlantic that the Orion CM must avoid during ascent aborts due to rough sea states and limited recovery capability.

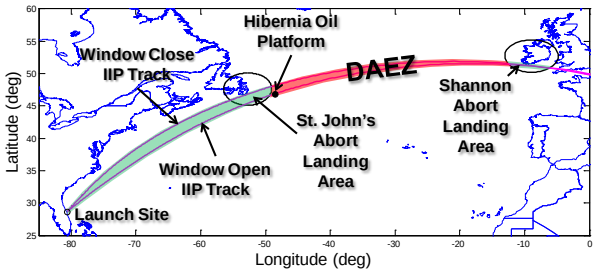

Figure 3. Orion DAEZ and Abort Landing Areas.

For launches at the close of the launch window, there are approximately 20 seconds of exposure to possible SM/DM impacts on Newfoundland. In-plane launches do not overfly Newfoundland. A similar exposure exists for launches at the open of the launch window which overfly the Hibernia Oil Platform off the coast of Newfoundland. Again, an in-plane launch alleviates the concern.

5.3.3 Abort Disposal Crew and Public Risk Trades: While disposal concerns existed and were quantified to some degree for the Constellation Program, no requirements for Ares Upper Stage or Orion component disposal existed within the program (at the time of cancellation) for failure or abort scenarios. While it was anticipated that the program would minimize public risk operationally when designing aborts, there was still a trade with crew safety versus public safety that needed to be analyzed. For example, if a performance anomaly occurred during ascent that resulted in a projected under-speed where debris could impact Eurasia, one option that could be considered involves shutting down the engine early to avoid the disposal concern. The resulting effect on the crew may be a longer or more performance limited burn that could result in a different insertion orbit and increase the risk to the crew. Many of these trades could be performed later for the final operational vehicles, but the Constellation Program performed analyses during the preliminary design cycle in order to feed back improvements into the design. The responsible AFSPC Range (i.e. 45th Space Wing) did not have the opportunity to complete a personnel and critical asset risk analysis for the downrange portion of a launch of the Ares vehicle prior to the cancellation of the program. Similar to the FTS delay time discussion, the system designers for future launch vehicles will need to work closely with the AFSPC range where the vehicle will be launched to ensure all public safety criteria set forth by the range are being met.

5.4 CM Raise Maneuver for Orion Reentry: For the vehicle reentry phase, all public safety responsibilities reside with the range user (e.g. NASA) in accordance with AFI 91-217 and the National Space Policy. To ensure public safety for nominal reentry, Orion is required to dispose of the service module and docking mechanism in the open ocean at least 25 nmi from U.S. land masses and 200 nmi from foreign land masses. The CM, drogue chutes, and other items jettisoned below 50,000 ft are required to impact within the primary landing zone around San Clemente, CA. In order to jettison the SM and DM early enough along the entry trajectory and still get the CM far enough downrange to hit the landing zone, a controlled CM downrange burn was inserted in to the entry timeline.

Notional reentry splashdown locations for the SM, DM, and CM are shown in Fig. 4 for both ascending and descending

approaches. The CM raise burn and lifting entry allow the CM to fly further downrange to the landing site, while the SM and DM fall through a steeper ballistic entry to an area outside the coastal keep-out zones.

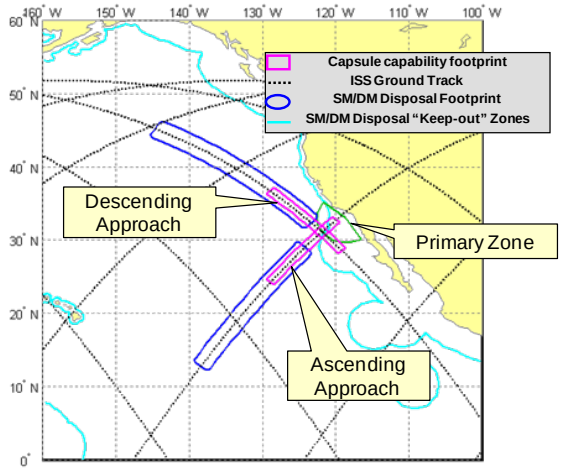

Figure 4. Notional reentry CM/SM/DM splashdown locations.

The CM raise burn was designed to reduce both public and crew risk by ensuring compliance with the 200 nmi disposal requirement while dropping the crew within the target landing zone. Without the burn, the crew and public risk splashdown requirements could not be concurrently met. The CM raise burn also reduced crew risk because CM to SM range at the anticipated time of SM aerodynamic break-up was increased. While more analysis was necessary on SM break-up dynamics, addition of the CM raise burn could only reduce the risk.

5.5 Ares First Stage Linear Shape Charge Extension: During the lifetime of the Space Shuttle Program, numerous risk assessments and sensitivity studies were performed to characterize the risk to the public for various failure scenarios during ascent. One such study conducted by the ER Safety office showed that approximately 80% of the overall risk, as quantified by the E_C estimate, was attributable to the lack of a Linear Shape Charge (LSC) on the aft segment of the Shuttle SRBs. This lesson learned was successfully carried forward into the Constellation Program which would utilize a five-segment version of the same solid rocket motor design for the first stage of the Ares vehicle. Early in the Constellation Program as part of the Ares I-X test flight, NASA and the 45th Space Wing personnel coordinated to ensure that the LSC was extended to include the aft segment of the booster. This new design was successfully implemented and flown on Ares I-X and was included in the baseline design for the crewed Ares launch vehicle that was being developed at the time.

The LSC extension was estimated to result in roughly the same 80% public risk reduction for Ares as was shown for the STS. In addition, a reduction in the risk to the crew was expected as well since the destruct lines for Ares would be less stringent, thereby allowing for more room to maneuver or recover from a vehicle malfunction before destruct action would need to be taken. This dramatic improvement to both public and crew safety was certainly worth the additional cost to incorporate the design change. Finally, the coordination between NASA and the ER during the LSC extension activity highlights the benefits of frequent discussions between the two organizations, particularly in the early design phase of the launch vehicle when modifications such as this one are easier and less costly to incorporate.

6. FAA LESSONS LEARNED

Analyses initiated after the *Columbia* accident demonstrated that a real-time system to track a launch or re-entry vehicle and activate aircraft hazard areas in the event of a catastrophic break-up may be necessary to provide a high level of aircraft protection without excessive impact on normal air-traffic patterns [20, 21]. In the wake of the *Columbia* accident, the FAA partnered with NASA to protect aircraft from potential Space Shuttle orbiter reentry hazards by using a set of procedures and tools that provide FAA air traffic managers and controllers with increased situational awareness before and during reentry missions. Past papers have described some of the key lessons that resulted from specific air traffic management needs, and many of the lessons learned were captured as requirements for a next-generation FAA tool that will provide similar capabilities during the planning and operational phases of the launches and reentries of future commercial space vehicles [22].

Even an upper-stage reentry break-up can produce risks that exceed U.S. consensus standards (e.g. above 1E-7 probability of an impact capable of causing a casualty) in areas of significant air-traffic [23]. Several U.S. agencies have collaborated on the development of aircraft vulnerability models and range safety standards that facilitate space transportation and mitigate the risk to aircraft from launch or reentry vehicle hazards [24]. The FAA continues to sponsor significant efforts, including tests and analyses, to develop such tools and standards because the optimal integration of space and air-traffic into the National Air Space requires rigorous measures that ensure the safety of occupants of all types of vehicles, as well as people on the ground.

The traditional ELV approach, which was codified in 14 CFR 417, uses a FTS designed and operated to protect populated (or otherwise protection) areas from debris impacts that exceed a ballistic coefficient of 3 psf. The traditional ELV approach includes Quantitative Risk Assessments (QRAs) to demonstrate compliance with consensus requirements to limit collective and individual risks to the public [5]. Since the traditional ELV approach does NOT entail an examination of the conditional risks to the public given an FTS activation event occurs, it could limit occupied vehicle flights and produce elevated risks for vehicle occupants even if the threat to the public is extremely low. The FAA's current RLV regulations (14 CFR Part 431) acknowledge that an FTS may not be optimal for some RLV missions, including crewed suborbital rockets. SpaceShipOne demonstrated that a relatively benign suborbital vehicle (without highly toxic or explosive propellants onboard) with a pilot can demonstrate compliance with the FAA's current public safety requirements for RLV missions without using a traditional flight termination system.

The first Dragon reentry mission demonstrated that the current collective public risk limit of no more the 30E-6 E_C due to debris from lift-off through landing is difficult to comply with for an orbital reusable vehicle [12]. Although the launch azimuth for that mission resulted in a fairly low risk to the public from launch, it corresponded to an orbital inclination

with a relatively high conditional risk given a failure that would lead to a random reentry [25]. The FAA estimated a relatively high expectation of casualty due to the possibility of a Dragon failure that would lead to a random reentry. Earlier studies showed that even a relatively mature orbital reusable vehicle would likely exceed FAA risk criteria due to potential debris hazards from lift off through landing for any coincident launch and landing point within the continental U.S. A more practical and common approach is to set separate risk limits of 100E-6 E_C for launch and 100E-6 E_C for reentry [5,26] as implemented in accordance with AFI 91-217 at AFSPC Ranges for all non-licensed (DoD/Civil) launches.

7. 45TH SPACE WING LESSONS LEARNED

7.1 Overall Probability of Failure and Allocation: Risk analysis is a process that is dependent upon mathematical models with many parameters that are used to simulate the consequences of vehicle failures and the resulting hazardous events. The models are approximations at various levels of sophistication and the model parameters are frequently difficult to quantify accurately. Consequently, the results of these studies can have considerable uncertainty. Even among the most proven models there can be significant differences in results when using the same set of input data. Thus, results from risk analysis programs have uncertainty coming from both the model designs and the model parameters. The two categories of uncertainty that occur in a risk analysis are aleatory and epistemic.

Aleatory uncertainty is the uncontrollable variability of events; typified by the distribution of debris impacts from one accident to another (the same initial conditions will not produce exactly the same consequences in sequential trials). In launch risk analysis models, the effect of aleatory uncertainty is most frequently averaged in the process of determining impact probability or expectation of casualty, E_C. In fact, E_C is the average number of casualties when considering all of the aleatory uncertainties.

Epistemic uncertainty is the uncertainty in the model and the model parameters. The model and parameters may contain inadequacies that introduce model or systematic uncertainty. If *epistemic* uncertainty is accounted for, then the computed E_C is no longer a point value but represented by a probability distribution. Epistemic (or model) uncertainty must account for any bias or conservatism in the model.

From a launch risk analysis point of view, aleatory uncertainty is the randomness in the occurrence and consequences of a launch accident (i.e. uncertainties that are irreducible). Epistemic uncertainty represents the uncertainty in the ability of the model to compute the true risk, and thus can be reduced by model improvements.

Failure probability uncertainty usually dominates the total uncertainty in a risk analysis for new vehicles. Uncertainty in the failure probability generally decreases as the vehicle matures, so the number of launches is an important factor. The occurrence of a failure is aleatory. The probability distribution describing the uncertainty in probability of failure can be used to reflect aleatory and epistemic sources of uncertainty.

Table 1. Uncertainties and Biases to be Considered in Launch Risk Analysis.

Uncertainty Description	Type of Uncertainty	Uncertainty Distribution Currently of Common Use	Bias	Effect on E_C Uncertainty	Comment
Failure probability	Failure probability is aleatory; its uncertainty is epistemic	Beta distribution most straight forward; changes with the number of launches	Most predictors are deliberately conservative	Dominant for new vehicles; less so as the vehicle matures	Must be evaluated by stage
Weighting of relative importance of previous flight success/failure experience	Epistemic	Currently not modeled	No intended bias	Not a major effect on Ec uncertainty	
Failure rate vs. time	Failure rate is aleatory; its uncertainty is epistemic	Currently not modeled	A bias vs. time is created if the failure rate vs. time is not modeled properly	Highest with stages having high failure probability	
Vehicle failure response mode (VFRM) allocation	Epistemic	Currently not modeled	No intended bias	Can have a big effect on Ec uncertainty	Manufacturer predictions of VFRM allocations seem to underestimate malfunction turn probability history
Discrete event failure probabilities	Aleatory	Currently not modeled	No bias	Depends upon the case	

Tab. 1 provides a summary of the uncertainties and biases associated with a vehicle failure probability that could be encountered when calculating the risk to personnel during a launch. The table also categorizes the sources, defines the uncertainty type and its bias for a probability of failure input parameter, and gives a general indication of the relative importance to the uncertainty in the computed risk.

The failure probability uncertainty model is better if it accounts for uncertainty levels separately in each of the stages or flight phases and for different failure modes. There is also the issue of the probability distribution of failure versus time. Failure probabilities can be biased because of conservative predictions by the AFSPC Range Safety office that governs the range a vehicle is launching from. Although the conservatism is appropriate in an analysis without uncertainty, it should be removed before making the uncertainty determination. The uncertainty analysis should be making an "unbiased estimate" of the average E_C and the uncertainty distribution of E_C. It has been the AFSPC Range Safety office's experience that range users have a tendency to under predict the failure probability of their vehicles when compared to empirical launch vehicle failure data. Since the range user does not have final authority for public safety on an AFSPC range, their developed overall vehicle probability of failure numbers have not been used by AFSPC Range Safety officials when calculating/assessing the risk to personnel and critical assets associated with any launch occurring on an AFSPC range. Instead AFSPC Range Safety officials calculate their own overall vehicle probability of failure rate and allocation for all vehicles launching from an AFSPC range, and use this value when assessing the risk to personnel and critical assets in accordance with the AFSPC range commander's safety program (AFPSCMAN 91-710).

For the Space Shuttle Program, the overall probability of failure published by NASA has at times differed from that of the ER Safety office by more than an order of magnitude. Over the 30-year course of the program, NASA and Air Force probability of failure estimates have slowly converged to a point where in January 2011, NASA published revised Space Shuttle reliability numbers that closely resembled the AFSPC derived failure rates that were used by the ER over the lifetime of the program. To address new launch vehicle development under the Constellation Program, additional discussions between NASA and the ER Safety office arose regarding the probability of failure estimation process. One such discussion that surfaced for the Ares I-X test flight involved trying to find a way to merge the best features of both the NASA bottom-up failure rate quantification process, which is based more on systems design, and the AFSPC top-down failure rate determination, which utilizes empirical launch vehicle failure data and is standardized for all launch vehicles. This series of discussions led to a new breakthrough in which a joint team from NASA and the 45th Space Wing developed a first flight adjustment methodology that bridged the gap between otherwise differing probability of failure estimates. "The method starts with the Air Force's generic failure probability estimate for first flight and adjusts the value based on the complexity of the vehicle as compared to the complexity of a generic vehicle. The results show an estimated vehicle average of 26% probability of failure versus 30% derived by the Common Standards Working Group [27], so there is relatively good agreement. The methodology used will continue to evolve [for future launch vehicles]" [28].

7.2 Crewed Space Flight Propulsive Systems: Based on past experience for both the Space Shuttle and Constellation Programs, it was evident to AFSPC Range Safety officials that liquid propulsion provides certain advantages over large solid rocket motors when trying to balance crew and public safety for crewed space flight. As discussed in section 5.2, changes proposed by the range user in an effort to increase crew survivability (e.g. removal of destruct ordinance, delaying destruct time, etc.) tend to increase the risk to personnel and critical assets in the launch area. For liquid propulsion launch vehicles, thrust can be terminated prior to activation of the FSS, thereby allowing for "extended" delay times to ensure crew safety without adversely affecting the safety of personnel and critical assets in the launch area or downrange overflight region.

Underscoring one of the advantages liquid propulsion has over large solid rocket motors for crewed space flight is a recent analysis completed by the AFSPC ER Safety office (45 SW/SE) showing that for "mature" vehicles FTS ordinance can be removed from the vehicle and a Thrust Termination System (TTS) is an acceptable FSS solution on the ER. Analysis shows that there is no increase in public safety and critical asset risk when comparing FTS vs. TTS for "mature" liquid propulsive vehicles. Removal of FTS ordnance from liquid vehicles will not only result in a cost reduction (~$1M/mission) and a slight increase in payload to orbit capability (~300 lbs), but it will also remove the inadvertent destruct concerns that exist in a crewed space flight program. Fig. 5 illustrates the differences between FTS destruct and a TTS solution.

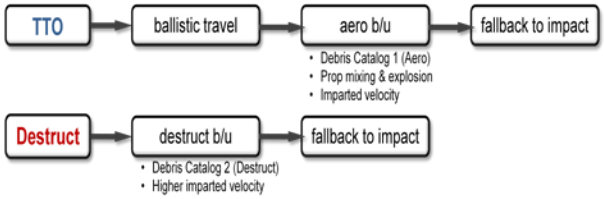

Figure 5. Differences between FTS methods.

Aside from the public safety considerations outlined here, the authors recognize that solid rocket motors offer some unique advantages versus liquid propulsion in other areas. The pros and cons of liquid versus solid rocket motors span numerous technical and non-technical discussions and are outside the scope of this paper.

7.3 Coordination between Government Agencies for Public Safety: Over the years, multiple government agencies, specifically AFSPC, NASA, and the FAA, have developed requirements and criteria in various documents that address launch vehicle public safety. There has been a concerted effort to ensure that launch vehicle public safety requirements and criteria recently published by NASA and the FAA mirror those that have been published by the governing AFSPC ranges for over 40 years. The result of this effort is multiple government agencies (AFSPC, NASA, and the FAA) enforcing public safety requirements on an AFSPC Range in support of crewed and non-crewed spaceflight. Prior to recently published NASA and FAA public safety requirements, a launch provider only had to meet AFPSC Range public safety requirements when launching a commercial, DoD, or civil mission from an AFSPC Range. Duplication of public safety requirements and roles/responsibilities is not an issue when launching from a non-AFSPC Range in that a launch operator launching any commercially licensed vehicle, whether crewed or non-crewed from a non-AFSPC range needs only to demonstrate compliance with FAA public safety requirements. While it is critically important to ensure consistency between federal agencies that govern and/or support U.S. domestic launch activity, it is also important to avoid duplicating efforts and/or imposing matching requirements that could result in potential waste and inefficiency when multiple agencies are involved in the launch of commercially licensed crewed/non-crewed vehicles from an AFSPC Range. During this early stage of developing commercial crew transport capabilities to low earth orbit, as well as for future civil launch vehicle development, proper coordination between federal agencies is essential. Once it has been determined that the involvement of multiple government agencies is necessary to ensure launch and reentry public safety from an AFSPC Range, the key lessons learned to avoid duplication and burdensome requirements can be summarized as follows:

1) establish an interagency forum, such as a range safety panel or the Common Standards Working Group, to facilitate coordinated safety related decision-making and approval processes, particularly to evaluate non-compliance requests or meets intent certifications, and
2) develop an approach to safety evaluations that accounts for the potentially different timetables used by each agency in the evaluation of compliance with their requirements.

7.3.1 NASA Public Safety Involvement at AFPSC Ranges: The purpose of Attachment A to NMI 1052.31, the

Webb/McNamara Agreement, 1963 [29], was to set forth the general concept of operations by DoD and NASA and to fix responsibilities for specific functions carried out at the ER (i.e. CCAFS/KSC) to include all downrange assets. This Agreement supersedes all other agreements, and where there are inconsistencies between other DoD/NASA agreements, provisions in the Webb/McNamara Agreement govern.

The DoD is the single manager responsible for the development, operation, and management of range facilities of the ER as a national asset, providing common range services to all missile and space vehicle launch programs of the DoD and NASA. In order to ensure a maximum of mutual assistance and a minimum of duplication, both DoD and NASA must inform each other of their plans and requirements and consult fully regarding their activities.

Range operation functions which are of such nature that any division of responsibility between agencies is impractical or undesirable is the responsibility of the DoD. The DoD is responsible for the following functions in support of operations of both DoD and NASA:

1) Control of ER resources during range operations and coordination with launch agency operations,
2) Flight/Public Safety,
3) Air Traffic Coordination, and
4) Sea Surveillance.

When launching from an AFSPC Range, NASA should review the AFSPC range governing document, AFSPCMAN 91-710, to ensure that their public safety requirements as contained in NPR 8715.5 are adequately captured in the overarching AFSPC range document. This was successfully done for the Constellation Program where NASA and 45th Space Wing personnel worked together through a range safety panel to create a joint tailored document that merged NPR 8715.5 and AFSPCMAN 91-710 as well as tailored the requirements to the specific vehicle being developed (i.e. Ares/Orion). During this process, it was evident that the vast majority of requirements in NPR 8715.5 were nearly identical to the corresponding requirement(s) listed in AFSPCMAN 91-710. The Webb/McNamara Agreement, written in 1963, made a concerted effort to minimize duplication between DoD and NASA and to define roles and responsibilities. Although NASA range safety program requirements outlined in NPR 8715.5 are certainly appropriate for ranges that NASA owns and operates, such as the Wallops Flight Facility, care should be taken to avoid unnecessary duplication for launches at ranges controlled and operated by AFSPC.

7.3.2 FAA Public Safety Involvement at AFPSC Ranges: As detailed in Section 2.2, FAA regulations focus on public safety requirements for commercially licensed launch vehicles because of the CSLAA of 2004. Currently there are no scheduled commercially licensed crewed space flights on the launch manifest at AFSPC ranges.

Per AFSPCI 10-1208 [30], paragraph 2.3.2, "cooperative involvement between 30 SW and 45 SW with FAA-licensed activities helps maintain the competitiveness of the US space industrial base in the world economy and promotes our national strength in space. AFSPC retains public safety and resource protection responsibilities for all activities on Vandenberg Air Force Base and Cape Canaveral Air Force Station." Paragraph 2.3.2 continues with, "for FAA-licensed launches, the FAA remains statutorily responsible for public health and safety, the safety of property, and national security or foreign policy interests of the United States under the CSLA. Additionally, the FAA-licensed company conducting the launch also retains responsibility for public safety of any launch it conducts from an AF range. Regardless of the type of activity (including FAA-licensed launches), AFSPC/CC, through his/her launch wing commanders, is responsible for the launch operation." In an attempt to detail roles and responsibilities of the Department of the Air Force and the FAA for overseeing safety of commercial space launch and reentry from AFPSC ranges the Under Secretary of the Air Force and the FAA Administrator signed a Memorandum of Agreement (MOA) for Space Transportation and Range Activities in 2007. One of the objectives of the AF/FAA MOA of 2007 is to minimize the regulatory burden on the U.S. commercial space sector by clearly delineating federal agency requirements, oversight responsibilities, and consolidating AF and FAA documentation products where possible, thereby precluding unnecessary overlap and duplication.

The AF/FAA MOA of 2007 includes a goal to ensure that common safety requirements exist for launches taking place at AFSPC ranges, but clearly this has proven difficult to achieve in practice because requirements tend to evolve at a different pace for each agency. Case in point, AFSPC ranges adopted a separate general public aggregated risk criteria of 100×10^{-6} E_C for launch and reentry with the publication of AFI 91-217 in February, 2010. AFI 91-217 simply incorporated aggregated risk criteria as detailed first in RCC 321-07, which was further updated to RCC 321-10. Currently the FAA regulations with risk acceptability criteria have not been updated and thus reflect an older standard [26]. Since FAA rule making is part of the Code of Federal Register changes to must abide by the Administrative Procedures Act, which involves public comments, etc. and take considerably more time than it takes the Air Force to change its requirements. In the meantime, commercially licensed launches, even from Air Force ranges, must follow the current FAA regulations. Thus, commercially licensed launches are currently held to a more restrictive criterion on AFSPC ranges when compared with non-licensed launches, i.e. DoD and civil (NASA) missions, unless a waiver is granted by the FAA.

The AF/FAA MOA of 2007 also states that the FAA will rely on AF safety processes for the review of all licensed launches from AF launch ranges for compliance with common safety requirements, provided that the FAA's LSSA of the AF launch ranges find that the AF safety process, procedures, and requirements implemented for each licensed launch satisfy FAA requirements, specifically 14 C.F.R. Ch III, Subchapter C, part 417. The FAA's LSSA of each AF launch range provides a basis for the FAA's reliance on the adequacy of the safety-related launch property and services provided by the AF to licensed launch operators. In essence, LSSAs are the FAA's mechanism for assessing the capabilities of the respective range safety organizations to protect public health and safety, when a range provides services to commercial launch companies. Once an LSSA has been completed the FAA does not duplicate analyses performed by the federal launch range according to approved processes. The FAA has issued an LSSA for the AFPSC ER, but in some cases has performed what could be considered duplicate risk analyses in order to meet the regulatory timetable for license evaluations, resulting in different risk estimates at various times during the safety evaluation process. An example of this is for the first Falcon 9/Dragon reentry mission. Just prior to launch when a complete set of final data were available, AFSPC Range (ER)

personnel performed a debris risk analysis from launch to orbital insertion that estimated an expectation of casualty that indicated compliance with FAA regulations. However, in order to make a license determination well in advance of the launch date, the FAA estimated the debris risk using only preliminary data that indicated potential non-compliance with the risk criteria used for licensing, such that a waiver was sought and granted [12]. Recognizing that input data and state-of-the-art methods often evolve over time, the FAA and ER have developed a process to jointly review and approve baseline risk analysis input data and methods that account for the different timetables used by each agency in their safety evaluations. For commercially licensed launches from the AFSPC ER both the FAA and ER will concur on a set of baseline risk analysis input parameters early in a launch flow. Once concurrence between the two organizations has been achieved AFSPC Range Safety personnel will complete the risk analysis for the commercially licensed launch in question. This analysis will then be used by both organizations to assess compliance with their respective requirements.

8. INNOVATIVE POTENTIAL APPROACH

Recent work done by the RCC Risk Committee outlined the steps involved in an innovative QRA approach that could provide a better balance between crew and public risk than the traditional ELV approach: "conditional risk management" for events that may involve a "safety intervention." The term "safety intervention" is used to encompass the entire range of risk mitigating actions that may be proposed for either Expendable Launch Vehicles (ELVs) or Reusable Launch Vehicles (RLVs), whether occupied or not. Activation of a FTS is an example of a common safety intervention for ELVs, and a contingency abort to an alternative landing site is an important safety intervention for an RLV.

Fig. 6 outlines a systematic QRA approach to manage risks associated with safety interventions developed by the RCC Risk Committee [5]. The sequence of steps shown in Fig. 6 was designed to assure completeness and avoid unnecessary efforts whenever possible. The figure shows the "conditional risk management approach" has two termination points. Step 12 is the final step if the analysis shows no potential for "high consequence events" and the probability of a safety intervention is determined *de minimis*. Step 13 is the last step if a complete analysis reveals the conditional risks from the safety intervention actions are acceptable.

The conditional risk management approach is intended to supplement the current risk management requirements of RCC 321-10 and assure that the proposed safety interventions address unacceptable levels of "high consequence" conditional risks and introduce reasonable conditional risks when the interventions actions are taken. Note that this Figure includes many undefined terms and criteria, such as a "remote" probability, "high consequence hazards," acceptable conditional collective and individual risks, etc. Even though "high consequences hazards" are not formally defined in the U.S. consensus standard for launch and reentry risk acceptability, these would obviously include hazards that could result in long term or irreversible consequences, such as public casualties, major environmental impacts, and negative impacts on the national security or foreign policy interests of the U.S. Even in the absence of consensus on important definitions of terms used in Fig. 6, the process shown can still be useful to evaluate the efficacy of a particular safety intervention if reasonable safety goals are accepted for a given launch or reentry vehicle. For example, if it was accepted that abort action should by planned to ensure (1) no more than 10% probability of casualty for occupants of a launch vehicle (people voluntarily exposed to risk), and (2) the conditional risks to the uninvolved public are three orders of magnitude lower than those voluntarily accepted by the vehicle occupants [31], then the design and operation of the vehicle should ensure that the uninvolved public are subject to no more than 0.1% probability of casualty given an abort action is implemented.

While the risk management process, including traditional QRAs and conditional risk analyses, may be useful in planning for contingency aborts, etc. for occupied launch or reentry vehicles, especially those under autonomous control, the design and operation of piloted vehicles should also account for longstanding rules governing emergency situations and decision-making theory as well. For example, in an in-flight emergency requiring immediate action, the pilot in command generally has been given the freedom to deviate from any requirement to the extent necessary to cope with the emergency, and later file a report to document the circumstances and rationale for that deviation. The history of aviation emergencies includes many cases where pilots have taken extraordinary measures to protect the public from a crash landing. Furthermore, acceptable safety mitigations should normally be expected to reduce the total and conditional risks relative to no mitigation. However, extenuating circumstances, such as national security or foreign policy interests, might warrant accepting higher safety risks from applying a safety mitigation compared to no mitigation.

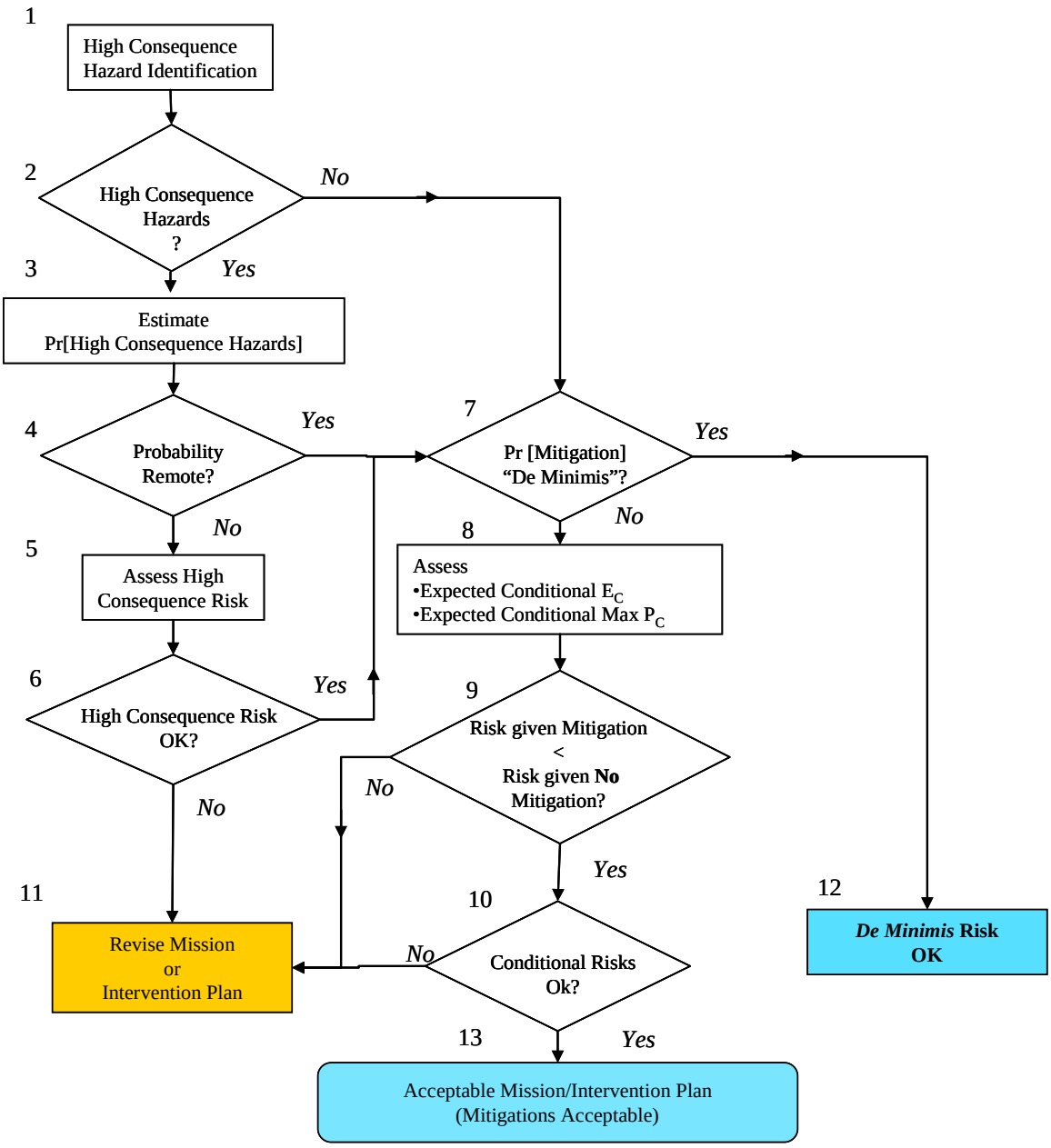

Figure 6. Conditional Risk Management Approach for Safety Interventions [5]

9. SUMMARY

This paper documents how the experiences of the development and operation of the Space Shuttle, as well as the preliminary design of the Constellation crew and launch vehicles, has proven that proper attention to range and crew safety requirements must be given early in the design phase to avoid additional operational complexities and ensure an optimal balance of risks to the public and people on-board. For example, unrealistic probability of launch abort estimates enabled certain Shuttle design features that placed crew and public safety at odds with each other. While these risks were eventually mitigated and balanced for the Space Shuttle Program, it required countless hours of effort to craft an acceptable set of operational rules and procedures. In addition, a truly optimal balance between crew and public safety could not be achieved without significant and costly redesigns. Examples from the Space Shuttle Program include the addition of a secondary impact limit line, the removal of the External Tank FTS, External Tank disposal for certain contingency aborts, and the compromised Orbiter flight rules for reentry. Abort planning analyses performed during the preliminary design phase for Constellation identified several areas where the design should address crew and public safety simultaneously. For example, the delay between activation of the launch abort vehicle (LAV) used to separate the crew vehicle from the launch vehicle and the termination of the launch vehicle flight should be designed to provide sufficient time for the LAV to depart the launch vehicle and achieve a safe separation distance, but not so much time that the launch vehicle chases down the LAV and destructs in close range, which can expose the crew vehicle to substantial risk from debris impacts. When employing a solid rocket motor propulsive system for a crewed mission any time delay in the activation of the FSS will result in additive risk to the general public. Recent AFSPC Range Safety analyses indicate that liquid propulsion provide an advantage over large solid rocket motors when integrating crew and public safety for crewed space flight because thrust can be terminated prior to activation of the flight safety system, thereby allowing for "extended" delay times to ensure crew safety without adversely affecting the safety of personnel and critical assets in the launch area or downrange over-flight region.

Another key lesson learned from the Shuttle and Constellation programs is that a vehicle developer should not establish crew safety design requirements or solutions in technical areas where crew and public safety intertwine without the involvement of the organization(s) responsible for public safety during launch and/or reentry. For example, the Constellation program found that if a performance anomaly occurred during ascent produced a projected under-speed where debris from the service module disposal could impact Eurasia, the engines might be shut down early to avoid the disposal debris risk to the public, but the result on the crew might be a longer crew capsule burn that could increase the risk to the crew. The Constellation program did not find a solution for that trade prior to cancellation; the AFSPC Range responsible for public safety was not yet engaged on that issue.

The increased activities involving crewed commercially licensed space transportation has highlighted the benefits of non-traditional approaches to safety. For example, the FAA's current RLV regulations acknowledge that a traditional FTS may not be optimal for some RLV missions, including crewed suborbital rockets. SpaceShipOne showed that a relatively benign suborbital vehicle (without highly toxic or explosive propellants onboard) with a pilot can demonstrate compliance with the FAA's current public safety requirements for RLV missions without using a traditional flight termination system. Along those same lines the AFSPC ER safety office has also recently completed an analysis that supports the removal of FTS ordnance from a "mature" liquid propulsive vehicle thereby allowing a TTS to be an acceptable FSS solution on the ER.

Recent experience where multiple government agencies are responsible for public safety during the launch/reentry of a commercially licensed crewed space vehicle indicates that duplication and potentially conflicting requirements must be avoided to the greatest extent possible. The responsible government agencies (AF, FAA, and NASA) have made a concerted effort to limit duplication by signing high-level agreements written specifically to address roles and responsibilities when launching any vehicle from an AFSPC Range. To further assist in the compliance and implementation of these agreements, each agency has worked cooperatively to ensure: 1) safety-related decision-making and approval processes, particularly when evaluating non-compliance requests or "meets intent" certifications, do not increase the work load imposed on a range user/licensee, and 2) AFSPC Range Safety offices complete safety evaluations/analyses in a timely manner so as to account for potentially different timetables used by each agency in the evaluation of compliance with their public safety requirements.

Current range safety requirements in the US are focused on ensuring public safety, but allow innovative approaches to integrate public and on-board safety, such as conditional risk management. Recent experience demonstrates that real-time systems and conditional risk management may be helpful in the integration of public and occupant safety. Analyses initiated after the *Columbia* accident demonstrated that a real-time system to track a launch or re-entry vehicle and activate aircraft hazard areas in the event of a catastrophic break-up may be necessary to provide a high level of aircraft protection without excessive impact on normal air-traffic patterns. A real-time system needs to manage conditional risks because the emergency event has occurred. RCC 321-10 has introduced a conditional risk management approach intended to supplement the current consensus risk management requirements and assure that safety interventions implemented (e.g. abort actions) produce reasonable conditional risks and address unacceptable levels of "high consequence" conditional risks.

10. REFERENCES

1. AFSPCI 91-701. *Launch Safety Program Policy.* June 2005.
2. AFSPCMAN 91-710. *Range Safety User Requirements Manual.* July 2004.
3. AFI 91-202. *The US Air Force Mishap Prevention Program.* August 2011.
4. AFI 91-217. *Space Safety and Mishap Prevention Program.* February 2010.

5. RCC Standard 321-10. *Common Risk Criteria Standards for National Test Ranges.* December 2010.

6. *Commercial Space Launch Act.* Title 51. U.S.C. Ch. 509. January 2011.

7. *MOA between the Department of the Air Force and Federal Aviation Administration on Safety for Space Transportation and Range Activities.* January 2001.

8. *Commercial Space Launch Amendments Act of 2004.* Public Law 108-492. 108th Congress. December 2004.

9. *Human Space Flight Requirements for Crew and Space Flight Participants.* Federal Register Vol. 71, No. 241. 14 CFR Part 460. December 2006. pp. 75616-75645.

10. *Licensing and Safety Requirements for Launch.* Federal Register Vol. 71, No. 165. 14 CFR Part 417. August 2006. pp. 50508-50727.

11. *Commercial Space Transportation Reusable Launch Vehicle and Reentry Licensing Regulations.* Federal Register Vol. 65, No. 182. 14 CFR Part 431. September 2000. pp. 56618-56667.

12. *Waiver of Acceptable Mission Risk Restriction for Reentry and a Reentry Vehicle.* Federal Register Vol. 75, No. 233. December 2010. pp. 75619-75621.

13. CCT-REQ-1130. *ISS Crew Transportation and Services Requirements Document.* April 2011.

14. NPR 8705.2B. *Subject: Human-Rating Requirements for Space Systems (w/change 1 dated 12/7/2009).* Office of Safety and Mission Assurance. May 2008.

15. Renzi, J. NSWC TR 88-216. *Space Shuttle Solid Rocket Boosters Destruct Analysis and Validation.* July 1988.

16. JSC-27848. *ET RSS Removal Analysis & Support.* May 1997.

17. NASA Shuttle Flight Rule A4-252. *Range Safety Policy.* Flight Rules Document Volume A, PCN-10. May 2009.

18. NASA Shuttle Flight Rule A2-207. *Landing Site Selection.* Flight Rules Document Volume A, PCN-10. May 2009.

19. NPR 8715.5A. *Subject: Range Flight Safety Program.* Office of Safety and Mission Assurance. September 2010.

20. *Determination of Debris Risk to the Public Due to the Columbia Breakup during Reentry.* Columbia Accident Investigation Board Report Volume II, Appendix D.16. October 2003.

21. Larson E., Wilde P., and Linn A. *Determination of Risk to Aircraft from Space Vehicle Debris.* 1st IAASS Symposium. Nice, France. October 2005.

22. Murray D.P. and Mitchell M. *Lessons Learned in Operational Space and Air Traffic Management.* AIAA-2010-1349. 48th AIAA Aerospace Sciences Meeting. Orlando, Florida. January 2010.

23. Ailor W. and P. Wilde. *Requirements for Warning Aircraft of Reentry Debris.* 3rd IAASS Safety Conference. Rome, Italy. October 2008.

24. Wilde P.D. and Draper C. *Aircraft Protection Standards and Implementation Guidelines for Range Safety.* AIAA-2010-1542. 48th AIAA Aerospace Sciences Meeting. Orlando, Florida. January 2010.

25. Patera R. *Hazard Analysis for Uncontrolled Space Vehicle Reentry.* Journal of Spacecraft and Rockets, Vol. 45, No. 5. September–October 2008.

26. Wilde P. *Public Risk Criteria and Rationale for Commercial Launch and Reentry.* 5th IAASS Symposium. Versailles, France. October 2011.

27. *Guide to Probability of Failure Analysis for New Expendable Launch Vehicles.* Version 1.0. FAA Commercial Space Transportation. November 2005.

28. CSMA-09-001. *Ares I-X Launch Area Risk Final Flight Data Package Scenario Probability Estimates.*

29. NMI 1052.31. *Webb/McNamara Agreement.* 1963.

30. AFSPCI 10-1208. *Spacelift Operations.* October 2008.

31. Starr, C. *Societal Benefit versus Technological Risk.* Science, Vol. 165. September 1969. pp.1232-1238.

11. ACRONYMS

AF	Air Force
AFI	Air Force Instruction
AFSPC	Air Force Space Command
AFSPC/CC	AFSPC Commander
AFSPCI	AFSPC Instruction
AFSPCMAN	AFSPC Manual
ATK	Alliant Techsystems Inc.,
CAIB	Columbia Accident Investigation Board
CCAFS	Cape Canaveral Air Force Station
CSLAA	Commercial Space Launch Amendments Act
CM	Crew Module
DAEZ	Downrange Abort Exclusion Zone
DM	Docking Mechanism
DoD	Department of Defense
E_C	Expected Casualties
ECAL	East Coast Abort Landing
ELV	Expendable Launch Vehicle
ER	Eastern Range
ET	External Tank
FAA	Federal Aviation Administration
FSS	Flight Safety System
FTS	Flight Termination System
High Q	high dynamic pressure
HQ	Headquarters
IIP	Instantaneous Impact Point
ILL	Impact Limit Line
KSC	Kennedy Space Center
LAS	Launch Abort System
LAV	Launch Abort Vehicle
LH2	Liquid Hydrogen
LoC	Loss of Crew
LOX	Liquid Oxygen

LSSA Launch Site Safety Assessments
LSC Linear Shape Charge
MAJCOM Major Command
MOA Memorandum of Agreement
MCC Mission Control Center
MECO Main Engine Cut-Off
MFCO Mission Flight Control Officer
NASA National Aeronautics & Space Administration
nmi nautical miles
NPR NASA Procedural Requirements
PC Probability of Casualty
psf pounds per square foot
QRA Quantitative Risk Assessment
RCC Range Commanders Council
RLV Reusable Launch Vehicle
RSS Range Safety System
RTS Range Tracking System
SM Service Module
SRB Solid Rocket Booster
SSME Space Shuttle Main Engine
STS Space Transportation System
SW/CC Space Wing Commander
TDTS Telemetry Data Transmitting Station
TTS Thrust Termination System
TVC Thrust Vector Control
U.S. United States

12. ACKNOWLEDGMENTS

The authors of this paper wish to thank the many participants from the NASA Johnson Space Center's Flight Dynamics Division, the 45th Space Wing's Safety Office, and the FAA's Office of Commercial Space Transportation for their continued support of crew and public safety discussions and integrated risk assessments. As a result of this cooperative effort between these three organizations, significant steps have been made to better understand the delicate balance between crew and public risk and communicate the need to integrate these two technical disciplines for future launch vehicle development.

Note: The views and opinions expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of any department or agency of the U.S. government. The employers of the authors neither approve nor disapprove of the contents of this paper.